SUBJECT: Regulating the provision of digital services to certain minors

COMMITTEE: Youth Health & Safety, Select — committee substitute recommended

VOTE: 5 ayes — Hull, Allison, Capriglione, Landgraf, Lozano

1 nay — Dutton

1 absent — T. King

2 present not voting — S. Thompson, A. Johnson

WITNESSES: For —Maurine Molak, David's Legacy Foundation; Danielle Greenup, Erik's Cause; Dawn Wible, Talk More. Tech Less; Cody Ivins, Texas Against Fentanyl; Brian Dixon, Texas Medical Association; Zachary Whiting, Texas Public Policy Foundation; Xiomi Oviedo, Unbound Now Austin; Jennifer Hogue; Kathy Johnson; Annie McAdams; Heather Schnelzer; Chloe Srinivasan (*Registered, but did not testify*: Rebecca Fowler, Mental Health America of Greater Houston; Judy Powell, Parent Guidance Center; Jill Sutton, Texas Osteopathic Medical Association; Suzi Kennon, Texas PTA; Jennifer Allmon, The Texas Catholic Conference of Bishops; Michelle Evans; Michael Hunsucker; Jackson Hunsucker; Thomas Parkinson)

Against — Kouri Marshall, Chamber of Progress; Antigone Davis, Meta; Andrew Kingman, State Privacy & Security Coalition; Servando Esparza, TechNet; John McCord, Texas Retailers Association; Mary Elizabeth Castle, Texas Values Action; Kevin Kane, YouTube (*Registered, but did not testify*: Christian Bionat, Greater Houston Partnership; Jonathan Covey, Texas Values Action)

On — Glenn Hamer, Texas Association of Business (*Registered, but did not testify*: Eric Marin, TEA)

DIGEST: CSHB 18 would require digital service providers to obtain consent from parents and guardians before known minors could enter into certain

agreements, give digital service providers certain duties when providing services to minors, and allow parents and guardians to take certain actions regarding a minor's data.

Definitions. CSHB 18 would define "digital service provider" as a person who owned or operated a website, application, program, or software that performed collections or processing functions with internet connectivity. The bill would define "known minor" as a child younger than 18 under circumstances in which a digital service provider had actual knowledge of or willfully disregarded a minor's age. A "verified parent" would be a person who had registered with a digital service provider as the parent or guardian of a known minor.

Agreements with known minors. A digital service provider could not enter into an agreement with a known minor unless the known minor's parent or guardian consented in a verifiable manner that was specific, informed, unambiguous, and occurred in the absence of any incentive. Acceptable methods a digital service provider could use to obtain consent would include:

- a form that the parent or guardian could sign and return by common carrier, facsimile, or electronic scan;
- a toll-free telephone number for the parent or guardian to call;
- a videoconferencing call with the parent or guardian;
- collecting information related to the parent or guardian's government-issued ID and deleting that information after confirming the identity of the parent or guardian;
- allowing the parent or guardian to consent through email and taking additional steps to verify the parent or guardian's identity; and
- obtaining consent from a person registered with the digital service provider as the known minor's verified parent or guardian.

Agreements would include terms of service agreements, user agreements, and the creation of an account for a digital service. An agreement would have to include a method for the known minor's parent or guardian to

register with the digital service provider as the minor's verified parent. Before obtaining consent from a known minor's parent or guardian, a digital service provider would be required to give the parent or guardian the ability to permanently enable settings to:

- enable the highest privacy setting that the digital provider offered;
- prevent the digital service provider from collecting any data associated with the minor that was not necessary to provide the service;
- prevent the digital service provider from processing any data associated with the minor in a way that was not related to the purpose for which the data was collected;
- prevent the digital service provider from sharing, disclosing, or transferring data associated with the minor in exchange for monetary or other valuable consideration;
- prevent the digital service provider from collecting geolocation data;
- disable targeted advertising for the minor; or
- prevent the minor from making purchases or financial transactions.

A digital service provider could not limit or discontinue a digital service provided to a known minor due to the parent or guardian's decisions regarding permanently enabling these settings.

If a minor's parent or guardian, including a verified parent, gave consent or performed another function under the provisions of the bill, the digital service provider would be considered to have actual knowledge that the child was less than 18 years old and would be required to treat the minor as a known minor.

Registration as a verified parent. Digital service providers would be required to provide a process for a known minor's parent or guardian to register with the provider as a verified parent. The registration process would require known minors' parents or guardians to confirm their identity using a method acceptable for consenting to an agreement. A person registered as a known minor's verified parent could give consent or

perform other functions of a known minor's parent or guardian relating to a digital service provider without confirming the verified parent's identity under provisions for consenting to an agreement.

Duty to prevent harm. Digital service providers would be required to exercise reasonable care to prevent physical, emotional, and developmental harm to a known minor relating to the minor's use of the digital service, including:

- self harm, suicide, eating disorders, and other similar behaviors;
- substance abuse and patterns of use indicating addiction;
- bullying and harassment;
- sexual exploitation, including enticement, grooming, trafficking, abuse, and child pornography;
- advertisements for products or services that are unlawful for minors, including illegal drugs, tobacco, gambling, pornography, and alcohol; and
- predatory, unfair, or deceptive marketing practices.

Digital service providers would have to exercise reasonable care to ensure that a known minor was not exposed to these types of harms related to the use of the digital service.

Access to data associated with known minors. A known minor's parent or guardian could submit a request to a digital service provider to access any data on the digital service associated with the minor. Digital service providers would have to make available a simple and easily accessible method for parents or guardians to make a request for access to the data. The method for the request would have to allow a known minor's parent or guardian to access:

- all data in the digital service provider's possession associated with the known minor, organized by type of data and the purpose for which the provider processed each type of data;
- the name of each third party to which the digital service provider disclosed the data, if applicable;

- each source other than the minor from which the digital service provider obtained data associated with the known minor;
- the length of time for which the digital service provider would retain the data;
- any index or score assigned to the minor as a result of the data, including who created the index and the manner in which the index was used;
- a method for the parent or guardian to dispute the accuracy of any data that the digital service provider collected or processed and request correction; and
- a method by which the parent or guardian could request the deletion of any data associated with the minor.

The method for requesting data would have to require parents or guardians to confirm their identity using the methods acceptable for consenting to an agreement. Verified parents would not be required to confirm their identity when making a request to a digital service provider with whom the parent was registered.

If a digital service provider received a dispute about the accuracy of data, the provider would have to determine whether the relevant data was inaccurate or incomplete and make necessary corrections within 45 days of receiving the dispute. If a digital service provider received a request to delete data associated with a known minor, the provider would have to do so within 45 days after the request was made.

Advertising and marketing duties. A digital service provider that allowed advertisements to known minors would have to disclose certain information in a clear and accessible manner at the time the advertisement was displayed, including:

- the name of the product, service, or brand;
- the subject matter of the advertisement or the marketing material;
- the reason each advertisement was targeted to a minor, if the digital service provider or advertisers targeted advertisements toward minors;

- how data associated with a known minor's use of the digital service led to each targeted advertisement; and
- whether certain media on the digital service were advertisements.

Use of algorithms. A digital service provider that used algorithms to automate the suggestion, promotion, or ranking of information to known minors on the digital service would be required to ensure that the algorithm did not interfere with its duty to prevent harm. A digital service provider also would have to clearly and accessibly disclose in its terms of service an overview of the way the digital service used algorithms to provide information to known minors and the way the algorithms used data associated with a known minor.

Applicability. The bill would not apply to state agencies, political subdivisions, financial institutions or data subject to certain federal laws, covered entities or business associates governed by certain federal laws and rules, small businesses as defined by the U.S. Small Business Administration, or higher education institutions.

Enforcement. A violation of the provisions of the bill would be a false, misleading, or deceptive act or practice. Remedies available under Business and Commerce Code ch. 17 subchapter E would be available for a violation of the bill.

The provisions of the bill would be severable. If any provision of the bill or its application to any person or circumstance were held invalid, the invalidity would not affect other provisions or applications that could be given effect without the invalid provision or application.

The bill would take effect September 1, 2024.

SUPPORTERS SAY:

CSHB 18, also known as the Securing Children Online through Parental Empowerment (SCOPE) Act, would improve online safety for minors. While federal law currently covers children under 12, minors of all ages are often exposed to harmful content online, which can put them in dangerous situations that affect their physical and mental health. The

current safeguards are not enough to protect children, and parents are not able to sufficiently monitor their children's online activities. The bill would protect children's data privacy by limiting online providers' ability to collect data from children. It also would empower parents to better protect their children and mitigate harm by giving them rights to their child's data.

The bill would not require digital service providers to reveal any source code for their algorithms. It would only require an overview of how the providers used the algorithms. Parents should be involved to ensure a child's safety whenever a website enters into an agreement with a minor.

While some have raised concerns about increased collection of sensitive information by digital service providers, the purpose of the bill would be to increase trust and reliability with those providers.

CRITICS SAY:

CSHB 18 would not necessarily achieve the goal of improving online safety for minors. Many companies already take steps to improve online safety for children and prohibit dangerous and violent content. Many factors contribute to mental health issues besides social media use.

The bill also could have the unintended consequence of increasing data collection by requiring more people to verify their identities.

Requiring companies to provide an overview of how digital providers used algorithms to provide information to minors could require those providers to provide information on how the algorithms identify and remove harmful content. Certain people could use this information to post more harmful content in the future.

The bill's definition of "digital service provider" is too broad and could encompass retail and other general use websites. The bill should apply only to websites that pose a higher risk of harm to children.